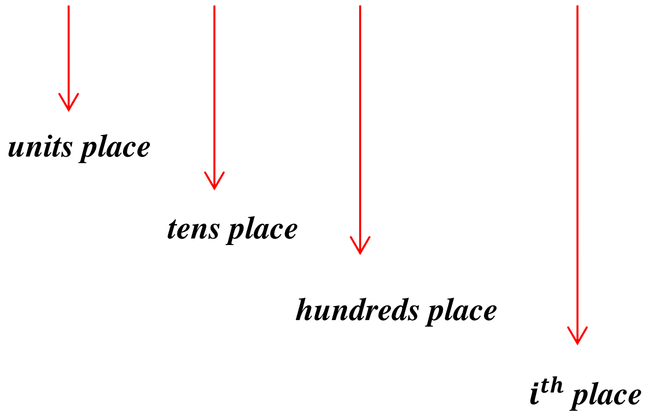
# SPECIAL DIVISIBILITY TETS

## DIVISIBILITY TEST

**(1)** Divisible by 2: If an integer is odd, then it is not divisible by 2. Thus, if an integer is even, then it is divisible by 2.

$$n = a_0 \text{ x } 10^0 + a_1 \text{ x } 10^1 + a_2 \text{ x } 10^2 + \ldots + a_k \text{ x } 10^k$$



Where $a_i$ is the digit on the $10^{ith}$ place of integer $n$.

***Example:*** $n = 246$ , $a_0 = 6$ is the digt on the $10^0 = 1$'s place of 246

$a_1 = 4$ is the digit on the $10^1 = 10$'s place of 246

$a_2 = 2$ is the digit on the $10^2 = 100$'s place of 246

- $n = 6 \text{ x } 10^0 + 4 \text{ x } 10^1 + 2 \text{ x } 10^2$

$\Rightarrow \quad n = 6 \text{ x } 1 + 4 \text{ x } 10 + 2 \text{ x } 100$

$\Rightarrow \quad n = 6 + 40 + 200$

$$\boxed{\boldsymbol{n = 246}}$$

For Divisibility Test by 2, check the last digit whether it is **odd** or **even**.

Observe that: $n = a_0 \text{ x } 10^0 + a_1 \text{ x } 10^1 + a_2 \text{ x } 10^2 + \ldots + a_k \text{ x } 10^k$ where $0 \leq a_1 \leq 9$.

$a_0$ x $10^0 = a_0$ x $1 = a_0 \equiv a_0 \ (mod\ 2)$ ***By Reflexive Property for Congruence***

$a_1$ x $10^1 = a_1$ x $10 = a_1$ x $0 \ (mod\ 2)$ ***By Transitive Properly for Congruence***

$a_2$ x $10^2 \equiv a_2$ x $(0)^2 \ (mod\ 2)$ ***By Transitive Properly for Congruence***

$\equiv 0 \ (mod\ 2)$ $\boldsymbol{a_2}$ **x** $\mathbf{0 = 0}$

.

.

.

$a_k$ x $10^k \equiv a_k$ x $(0)^k \ (mod\ 2)$ **By Transitive Property for Congruence**

$\equiv (mod 2)$ $\boldsymbol{a_k}$ **x** $\mathbf{0 = 0}$

**(2)** Divisible by 3: An integer is divisible by 3 if the sum of its digits is divisible by 3.

Observe we that:: $n = a_0$ x $10^0$ + $a_1$ x $10^1$ + $a_2$ x $10^2$ + … + $a_k$ x $10^k$

$10^0 = 1 \equiv 1 \ (mod\ 3)$ ***By Reflexive Property for Congruence***

$10^1 = 10 \equiv 1 \ (mod\ 3)$ ***By Congruence Classes Modulo 3***

$\mathbf{13 = 10 = 7 = 4 = 1} \ (\boldsymbol{mod}\ \mathbf{3})$

$10^2 \equiv (1)^2 \ (mod\ 3)$ **By Congruence Property If** $\boldsymbol{a \equiv b \ (mod\ m)}$**,**

**then** $\boldsymbol{a^n \equiv b^n \ (mod\ m)}$

$\equiv 1 \ (mod\ 3)$ $(\mathbf{1})^2 = \mathbf{1}$

.

.

.

$10^k \equiv (1)^k \ (mod\ 3)$ **By Congruence Property If** $\boldsymbol{a \equiv b \ (mod\ m)}$**,**

**then** $\boldsymbol{a^n \equiv b^n \ (mod\ m)}$

$\equiv 1 \ (mod\ 3)$

$n \equiv (a_0 \text{ x } 1) + (a_1 \text{ x } 1) + (a_2 \text{ x } 1) + \ldots + (a_k \text{ x } 1)\ (mod\ 3)$

$\boldsymbol{n \equiv a_0 + a_1 + a_2 + \ldots + a_k\ (mod\ 3)}$

## LINEAR CONGRUENCES

***Definition:*** A congruence of the form $ax \equiv b\ (mod\ n)$ where $x$ is an unknown integer, is called a LINEAR COUGEUNICE IN THE VARIABLE $x$.

- ⇨ A solution to this Linear Congruence is an integer $x_0$, such that $ax_0 \equiv b\ (mod\ m)$.
- ⇨ Note that if $x_0$ is a solution to the linear congruence and $x \equiv x_0\ (mod\ m)$, then $x$ is also a solution. This means that if one member of a congruence class modulo $m$ is a solution, then all the members of this class are solutions.

Example: Solve $4x \equiv 2\ (mod\ 6)$.

- $x \equiv 0\ (mod\ 6)$

⇒ $4.x \equiv 4.0\ (mod\ 6)$

⇒ $4x \equiv 0\ (mod\ 6)$

- $x \equiv 1\ (mod\ 6)$

⇒ $4.x \equiv 4.1\ (mod\ 6)$

⇒ $4x \equiv 4\ (mod\ 6)$

- $x \equiv 2\ (mod\ 6)$

⇒ $4.x \equiv 4.2\ (mod\ 6)$

⇒ $4x \equiv 8\ (mod\ 6)$

$\Rightarrow \quad \boxed{4x \equiv 2\ (mod\ 6)}$

- $x \equiv 3\ (mod\ 6)$

$\Rightarrow \quad 4.x \equiv 4.3\ (mod\ 6)$

$\Rightarrow \quad 4x \equiv 12\ (mod\ 6)$

$\Rightarrow \quad 4x \equiv 0\ (mod\ 6)$

- $x \equiv 4\ (mod\ 6)$

$\Rightarrow \quad 4.x \equiv 4.4\ (mod\ 6)$

$\Rightarrow \quad 4x \equiv 16\ (mod\ 6)$

$\Rightarrow \quad 4x \equiv 4\ (mod\ 6)$

- $x \equiv 5\ (mod\ 6)$

$\Rightarrow \quad 4.x \equiv 4.5\ (mod\ 6)$

$\Rightarrow \quad 4x \equiv 20\ (mod\ 6)$

$\Rightarrow \quad \boxed{4x \equiv 2\ (mod\ 6)}$

$$\boxed{\begin{array}{c} x \equiv 2\ (mod\ 6) \\[1em] x \equiv 5\ (mod\ 6) \end{array}} \quad \begin{array}{c} \longrightarrow \quad x \equiv 8\ (mod\ 6) \\[1em] \longrightarrow \quad x \equiv 11\ (mod\ 6) \end{array}$$

$\hookrightarrow$ Solutions for $4x \equiv 2\ (mod\ 6)$

The following theorem tells us when a linear congruence in one variable has solutions and if it does, tells exactly how many INCONGRUENT SOLUTIONS there are mod $m$.

***Theorem 1:*** The linear congruence $ax \equiv b\ (mod\ m)$ has a solution if only if $(a, m)|b$.

***Theorem 2:*** Let $(a, m) = d$. If $d|b$, then $ax \equiv b\ (mod\ m)$ has $d$ mutually incongruent solutions modulo $m$.

Example: $4x \equiv 2\ (mod\ 6)$.

- $(a, m)|b$

$\Rightarrow\ (4, 6)|2$

$\Rightarrow\ \boxed{\mathbf{2|2}}$

Therefore, $4x \equiv 2\ (mod\ 6)$ has a solution. Also, the latter has $d = 2$ mutually incongruent solutions modulo 6.

That is:

$$\boxed{\left.\begin{array}{l} x \equiv 2\ (mod\ 6) \\ x \equiv 5\ (mod\ 6) \end{array}\right\} \quad 2 \not\equiv 5\ (mod\ 6)}$$

***Corollaries:***

(1) Let $d = (a, m)$ and $d|b$. The incongruent solutions to $ax = b\ (mod\ m)$ are:

$$\boxed{X_0, X_0 + \frac{m}{d}, X_0 + \frac{2m}{d}, \ldots, X_0 + \frac{m(d-1)}{d}}$$

(2) If $(a, m) = 1$, then the linear congruence $ax \equiv b\ (mod\ m)$ has a unique solution modulo $m$.

***Example 1:*** Solve $4x \equiv 2\ (mod\ 6)$.

***Solution:*** From $ax \equiv b\ (mod\ m)$, $a = 4$; $b = 2$; $m = 6$.

So that:

- $(a, m)|b$

$\Rightarrow \ (4,6)\ 12 \ \rightarrow \ 2|2$

***Therefore, there are $\boldsymbol{2}$ incongruent solutions modulo $\boldsymbol{6}$.***

Then it follows that:

- $4x \equiv 2 \ (mod\ 6)$

$\Rightarrow \ 2x \equiv 1 \ (mod\ 6)$ ***Using the Theorem: If $\boldsymbol{ca \equiv cb\ (mod\ m)}$, and $\boldsymbol{(c,m) = d}$, then $\boldsymbol{a \equiv b\ (mod\ \frac{m}{d})}$***

$\Rightarrow \ 2x \equiv 4 \ (mod 3)$ ***Congruence Classes modulo 3; $\boldsymbol{1 \equiv 4\ (mod 3)}$***

$\Rightarrow \ \boxed{x \equiv 2 \ (mod 3)}$ ***Using the Theorem: If $\boldsymbol{ca \equiv cb\ (mod\ m)}$ and $\boldsymbol{(c,m) = 1}$, then $\boldsymbol{a \equiv b\ (mod\ m)}$***

By Corollary 1, $x \equiv 2 \ (mod\ 6)$ is a solution to the linear congruence $4x \equiv 2 (mod\ 6)$ and the other incongruent solution is:

- $x = x_0 + \frac{m}{d}$

$\Rightarrow \ x = 2 + \dfrac{6}{2}$

$\Rightarrow \ x = 2 + 3$

$\Rightarrow \ \boxed{x = 5} \ \Longrightarrow \ \boxed{x \equiv 5 (mod\ 6)}$

So two incongruent solutions to the linear congruence $4x \equiv 2 \ (mod\ 6)$ are:

$$\boxed{\begin{array}{l} x \equiv 2 \ (mod 6) \\ x \ \equiv 5 \ (mod\ 6) \end{array}}$$

## CHINESE REMAINDER THEOREM

Let $m_1, m_2, \ldots, m_k \in \mathbb{N}$ *such that* $(m_i, m_j) \ = \ 1$ for $i \neq j$.

Then the system of linear congruence's

$$\boxed{\begin{aligned} x &\equiv a_1 (mod\ m_1) \\ x &\equiv a_2\ (mod\ m_2) \\ &\ \ \vdots \\ x &\equiv a_k\ (mod\ m_k) \end{aligned}}$$

Has a simultaneous solution which is unique modulo $m_1, m_2, m_3 \ldots, m_k$.

***Example 2:*** Find a number which leaves a remainder $2,3,2$ when divided by $3,5,7$ respectively. So, by Chinese Remainder Theorem, we have system of linear congruence's:

$$\boxed{\begin{aligned} x &\equiv 2\ (mod\ 3) \\ x &\equiv 3\ (mod\ 5) \\ x &\equiv 2\ (mod\ \ 7) \end{aligned}}$$

***Solution:*** Since $3, 5$ *and* $7$ are primes then $3, 5,$ *and* $7$ are co primes, so, by Chinese Remainder Theorem, there is a simultaneous solution $modulo$ $(3)\ (5)\ (7)\ = 105.$

$$\left\{\begin{array}{ll} x \equiv 2\ (mod\ 3) & (3,5) = 1 \\ x \equiv 3\ (mod\ 5) & (3,7) = 1 \\ x \equiv 2 (mod\ 7) & (5,7) = 1 \end{array}\right\} \quad \text{unique solution} \quad (3)(5)(7) = 105.$$

- From the 1st Congruence:

  - $x \equiv 2\ (mod\ 3)$ ***By Definition of Congruence***

$\Rightarrow\ 3 |\ (x - 20)$ ***By Definition of Divisibility***

$\Rightarrow\ x - 2 + 2 = 3n + 2$ ***Add 2 to both sides Equation***

(1) $\Rightarrow\ \boxed{x\ =\ 3n + 2}$ $\boldsymbol{LHS: -2 + 2\ = 0}$

- Then the 2nd Congruence:
  - $x \equiv 3 \ (mod\ 5)$

$\Rightarrow \quad 3n + 2 = 3(mod\ 5)$ ***Substituting the value of x from equation (1)***

$\Rightarrow \quad 3n + 2 \pm 2 \equiv (mod\ 5)$ ***Adding $-2$ to both sides of the Congruence***

$\Rightarrow \quad 3n \equiv 1 \ (mod\ 5)$ $\mathbf{2 + -2 = 0 \ \textit{and} \ 3 + -2 = 1}$

$\Rightarrow \quad 3n \equiv 6 \ (mod\ 5)$ ***By Transitive Property for Congruence***

$\Rightarrow \quad n \equiv 2 \ (mod\ 5)$ ***Divide both sides of the Congruence by $\mathbf{3}$ by Theorem: If $\boldsymbol{ca = \ cb \ (mod\ m)}$ and $\boldsymbol{(cm) = 1, then\ a \equiv b \ (mod\ m\ )}$***

$\Rightarrow \quad 5|\ (n - 2)$ ***By Definition of Congruence***

$\Rightarrow \quad n - 2 = 5m, m \in \mathbb{Z}$ ***By Definition of Divisibility***

$\Rightarrow \quad n - 2 + 2 = \ 5m + 2$ ***Add 2 to both side of the Congruence***

(2) $\Rightarrow \quad \boxed{n = 5m + 2}$ ***Since $\mathbf{-2 + 2 = 0}$***

- Back to Equation (1), we have:
  - $x \ = 3n + 2$

$\Rightarrow \quad x = 3\ (5m + 2) + 2$ ***Substituting the value of $\mathbf{n}$ from Equation(2)***

$\Rightarrow \quad x \ = (15m + 6) + 2$ ***By Distributive Property for Multiplication over Addition***

$\Rightarrow \quad x \ = 15m + (6 + 2)$ ***By Associative Property for Addition***

(3) $\Rightarrow \boxed{x = 15m + 8}$ *Since* $\mathbf{6 + 2 = 8}$

- For the 3rd Congruence:
  - $x \equiv 2 \ (mod\ 7)$

$\Rightarrow 15m + 8 \equiv 2 \ (mod\ 7)$ *Substituting the value of x from Equation (3)*

$\Rightarrow 15m + 8 + -8 \equiv 2 + -8 \ (mod\ 7)$ *Add* $\mathbf{8}$ *to both sides of the Congruence*

$\Rightarrow 15m \equiv -6 \ (mod\ 7)$ *Divide both sides of the congruence by* $\mathbf{3}$ *by Theorem: Is* $\boldsymbol{ca = cb \ (mod\ m)}$ *and* $\boldsymbol{(c, m) = 1)}$, *then* $\boldsymbol{a = b \ (mod\ m)}$.

$\Rightarrow 5m \equiv -2 \ (mod\ 7)$ *Since* $\mathbf{8 + -8 = 0}$ *and* $\mathbf{24 - 8 = -6}$

$\Rightarrow 5m \equiv -2 + 7 \ (mod\ 7)$ *By Congruence Classes mod* $\mathbf{7}$ *(add* $\mathbf{7}$ *to* $\mathbf{-2}$*)*

$\Rightarrow 5m \equiv 5 \ (mod\ 7)$ *Since* $\mathbf{-2 + 7}$

$\Rightarrow m \equiv 1 \ (mod\ 7)$ *Divide both sides of the Congruence by 5 by Theorem:* $\boldsymbol{If\ ca \equiv cb \ (modm) and \ (cm) = 1}$ *then* $\boldsymbol{a \equiv b(modm)}$.

$\Rightarrow 7 | (m - 1)$ *By Definition of Congruence*

$\Rightarrow m - 1 = 7r, r \in \mathbb{Z}$ *By Definition of Divisibility*

$\Rightarrow m - 1 + 1 = 7r + 1$ *Add* $\mathbf{1}$ *to both sides of the Equation*

(4) $\Rightarrow \boxed{m = 7r + 1}$ *Since* $\mathbf{-1 + 1 = 0}$

- Back to Equation (3):
  - $x = 15m + 8$

| | |
|---|---|
| $\Rightarrow \; x = 15\,(7r + 1) + 8$ | ***Substituting the value of $\mathbf{m}$ from Equation (4)*** |
| $\Rightarrow \; x = (105r + 15) + 8$ | ***By Distributive Property for Multiplication over Addition*** |
| $\Rightarrow \; x = 105r + (15 + 8)$ | ***By Associative Property for Addition*** |
| $\Rightarrow \; x = 105r + 23$ | ***Since $\mathbf{15 + 8 = 23}$*** |
| $\Rightarrow \; x + - 23 = 105r + 23 - 23$ | ***Add $\mathbf{-23}$ to both sides of the Equation*** |
| $\Rightarrow \; x - 23 = 105r$ | ***LHS: By Definition of Subtraction*** |
| $\Rightarrow \; 105 \mid (x - 23)$ | ***RHS: $\mathbf{23 + -23 = 0}$*** |
| $\Rightarrow \; 105 \mid (x - 23)$ | ***By Definition of Divisibility*** |
| $\Rightarrow \; \boxed{x \equiv 23 \; (mod\ 105)}$ | ***By Definition of Congruence*** |

Check:

| | | | |
|---|---|---|---|
| $x \equiv 2 \; (mod\ 3)$ | $\longrightarrow$ | $23 \equiv 2 \; (mod\ 3)$ | $For\ 23 = 3\,(7) + 2$ |
| $x \equiv 3 \; (mod\ 5)$ | $\longrightarrow$ | $23 \equiv 2 \; (mod\ 5)$ | $For\ 23 = 5\,(4) + 3$ |
| $x \equiv 2 \; (mod\ 7)$ | $\longrightarrow$ | $23 \equiv 2 \; (mod\ 7)$ | $For\ 23 = 7\,(3) + 2$ |

Thus, $\boxed{x \equiv 23 \; (mod\ 105)}$ is the unique solution for the system of Linear Congruence

$$\left\{ \begin{array}{l} x \equiv 2 \; (mod\ 3) \\ x \equiv 3 \; (mod\ 5) \\ x \equiv 2 (mod\ \ 7) \end{array} \right.$$